Department of Homeland Security Daily Open Source Infrastructure Report for 26 December 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Department of Homeland Security on Friday, December 22, made available for public review an aggressive and comprehensive set of proposed regulations that will improve security at high−risk chemical facilities nationwide. (See item 6)
- The Port Authority of New York and New Jersey, in an analysis based on work by Lawrence Livermore National Laboratory and the Rensselaer Polytechnic Institute, has revised an earlier assessment of the PATH system and now states that the tunnels are structurally more vulnerable than first thought. (See item 18)
- The Savannah Morning News reports the Savannah−Chatham Metropolitan Police Bomb Squad seized several canisters containing explosive−making materials, including German military grenades, igniters, fuses, and consumer fireworks, from Skidaway Mobile Estates in Georgia. (See item 44)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *December 22, Bloomberg* — **TransCanada to buy El Paso pipeline for $3.4 billion.** TransCanada, Canada's biggest pipeline company, and its U.S. affiliate agreed to buy

natural−gas pipelines and storage facilities from El Paso Corp. for about $3.4 billion in cash, a move that will expand the Canadian company's network by about 40 percent. Houston−based El Paso is selling its ANR Pipeline Co., storage facilities in Michigan and a stake in another line to cut debt and improve its creditworthiness. ANR Pipeline is a 10,500 mile system that delivers gas from producing regions in Louisiana, Texas, and Oklahoma to population centers in Illinois, Ohio, and other Midwest states. The acquisitions will lengthen TransCanada's pipeline network to more than 35,600 miles and will nearly triple its capacity to store the fuel, which has been subject to wide swings in price, to 360 billion cubic feet.
Source: http://www.bloomberg.com/apps/news?pid=20601072&sid=aJaT12J56A64&refer=energy

2. *December 21, Associated Press* — **Some Indian Point workers afraid to raise safety issues, NRC says.** Some workers at the Indian Point nuclear power plants are reluctant to raise safety concerns because they fear retribution, the Nuclear Regulatory Commission (NRC) said Thursday, December 21. During an inspection in September, "We found out that there were workers who perceived that they would be treated negatively by management for raising issues and consequently some of the workers expressed reluctance to raise issues under certain circumstances," said NRC spokesperson Neil Sheehan. An NRC report, sent Thursday to Indian Point owner Entergy Nuclear Northeast, found that most workers said they would not hesitate to raise issues they believed involved nuclear safety. But the results still had nuclear safety implications, it said. The NRC report criticized Entergy for not acting on "chilling" issues raised last year and earlier this year. The commission also announced Thursday that it has renewed a "deviation memo" for Indian Point that allows it to closely scrutinize Indian Point in 2007. Sheehan said the primary reasons were Indian Point's problems with groundwater contamination and faulty emergency sirens.
Source: http://www.silive.com/newsflash/metro/index.ssf?/base/news−22/1166729646180800.xml&storylist=simetro

3. *December 21, Federal Energy Regulatory Commission* — **FERC approves revised $1 billion Millennium Pipeline Project to bring new gas service to the northeast.** The Federal Energy Regulatory Commission (FERC) Thursday, December 21, approved a $1.04 billion interstate natural gas pipeline project proposed by five companies that will provide Canadian and domestic gas to meet rising energy demand in New York. The project is proposed by the Millennium Pipeline Co, Columbia Gas Transmission, Empire State Pipeline and Empire Pipeline, Algonquin Gas Transmission, and Iroquois Gas Transmission System LP. The companies propose to construct and operate more than 260 miles of new pipeline and more than 115,130 horsepower of compression to transport natural gas from the U.S.−Canada border to the New York City metropolitan region. FERC Chairman Joseph T. Kelliher observed: “The Millenium pipeline is an important project. It will help deliver badly needed natural gas supplies to the New York City metropolitan area.” The Commission previously approved the original Millennium Pipeline Project in an order issued September 19, 2002. However, the project was never built after failing to obtain necessary regulatory approval from the State of New York. Shippers for the new service include Consolidated Edison Co. and KeySpan Gas East Corp., among others.
Chairman's Statement: http://www.ferc.gov/press−room/statements−speeches/kelliher/2006/12−21−06−kelliher−C−1.asp
Decision: http://www.ferc.gov/whats−new/comm−meet/122106/C−1.pdf

Source: http://www.ferc.gov/press−room/press−releases/2006/2006−4/12 −21−06−C−1.asp

4. *December 20, Mohave Daily News (AZ)* — **Rash of copper wire thefts hits Tri−state even as prices drop.** Allen Stone Barnes and Sabrina Andrea Carlsrud are charged in the alleged break−in and theft of copper wire at the Western Area Power Administration substation in Mohave Valley, AZ. Barnes and Carlsrud are also suspects in the Tuesday, December 19, break−in and theft of copper wire from the Unisource Energy Service's Boundary Cone substation. At Carlsrud's residence were 100 pounds of copper wire believed stolen from the Unisource substation. At the WAPA power station, someone had cut a hole in the fence and power lines and transformers had been damaged. Estimates are about $10,000 in damages. The Unisource substation was shut down for about two hours; about 500 customers lost power. A Unisource warehouse and another substation under construction were also vandalized several months ago and copper wire was stolen. Copper prices almost tripled statewide about two months ago, however, copper prices have since dropped dramatically. Other recent thefts include copper ground wire from a Mohave Electric Cooperative substation in Bullhead City and an Aha Macav Power Service substation in Mohave Valley. Bill Syr of the Aha Macav Power Service said thieves have stolen copper wire from more than 200 ground poles at that substation in the past six weeks.
Source: http://www.mohavedailynews.com/articles/2006/12/21/news/loca l/local3.txt

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *December 23, Burlington County Times (NJ)* — **Chlorine leak at water−treatment plant closes nearby buildings.** Three workers were hospitalized and two buildings on the Deborah Heart and Lung Center campus in Burlington County, NJ, were closed Friday, December 22, following a chlorine leak at the water−treatment plant that serves the hospital, officials said. The liquid chlorine leak was discovered Friday morning in a water−treatment building on Trenton Road. Firefighters responded, but the small leak already had been contained and fixed by hospital maintenance workers. A short time later, however, employees in the nearby Cymrot Administration Building reported a strong odor of chlorine. The building is approximately 30 feet from the water treatment plant. The administration building was evacuated and 18 workers were examined for possible chemical exposure. Three of those workers were taken to Virtua Memorial Hospital Burlington County in Mount Holly for observation because they complained of dizziness. A Burlington County hazardous−materials handling team went to the hospital, determined there was no additional leakage, and declared both buildings safe. Both buildings remained closed Friday as a precaution.
Source: http://www.phillyburbs.com/pb−dyn/news/112−12232006−951919.h tml

6. *December 22, Department of Homeland Security* — **DHS introduces new regulations to secure high−risk chemical facilities.** The Department of Homeland Security (DHS) on Friday, December 22, made available for public review an aggressive and comprehensive set of proposed regulations that will improve security at high−risk chemical facilities nationwide. The proposed regulations are expected to be published in the Federal Register as an Advanced Notice of Rulemaking and will be available for public comment until February 7, 2007. The proposed regulations require that chemical facilities fitting certain profiles complete a secure

online risk assessment to assist in determining their overall level of risk. High−risk facilities will then be required to conduct vulnerability assessments and submit site security plans that meet the department's performance standards. The department will validate submissions through audits and site inspections, and will provide technical assistance to facility owners and operators as needed. Performance standards will be designed to achieve specific outcomes, such as securing the perimeter and critical targets, controlling access, deterring theft of potentially dangerous chemicals, and preventing internal sabotage. Security strategies necessary to satisfy these standards will depend upon the level of risk at each facility.
Source: http://www.dhs.gov/xnews/releases/pr_1166807052891.shtm

7. *December 22, Press−Enterprise (CA)* — **Train derails, spills chemicals in California.** A freight train hauling hazardous materials derailed Friday afternoon, December 22, in San Bernardino County's High Desert, spilling between 50 and 200 gallons of flammable liquids and leaving dozens of cargo containers in a tangled heap. The 80−car BNSF Railway train was bound from Chicago to Los Angeles when a dozen cars derailed near the remote town of Newberry Springs, CA. Dozens of emergency responders initially believed between 20 to 30 cars had left the tracks, but many of the train's cars were stacked with two or more cargo containers, giving the appearance that more cars derailed. The train's paperwork showed that some of the cars were carrying 55−gallon drums of toluene and naphtha. The railroad estimated about 50 gallons of liquid was spilled, but Fire Chief Lance Milanez estimated the spill at about 200 gallons. He said that two of the cars that derailed contained flammable liquid. One spilled what appeared to be toluene. The track would remain shut down to other trains until the derailed cars were moved away in trucks and locomotives pulled away the remaining cars.
Source: http://www.pe.com/localnews/inland/stories/PE_News_Local_B_bderail23.3a4f342.html

[Return to top]

Defense Industrial Base Sector

8. *January 01, National Defense* — **Investments in unmanned aircraft focus on ground operators.** Current and future purchases of unmanned aircraft increasingly are taking into account grounds troops' demand for timely intelligence in a user−friendly format. Consequently, the military services are turning more attention and funding to the devices used to program and operate the aircraft, officials assert. Typically, 90 percent of the dollars spent on unmanned systems are invested directly into the platform while only 10 percent goes to the command and control system, says Mark Bigham, business development director at the Raytheon Company. The lack of user−friendly standards for current ground control stations not only make it harder for operators to fly unmanned aerial vehicles (UAV), but also results in mishaps. One of the biggest contributing factors to crashes and failures in UAVs stems from human error, according to a Federal Aviation Administration study. The study implicates poorly designed user interfaces on ground control stations as a cause for human error. For troops on the battlefield looking at UAV video streams remotely, the problem is not the interface, but understanding the source of the information, and correlating the data to the correct position on the ground.
Source: http://www.nationaldefensemagazine.org/issues/2007/January/InvestmentsInUnmanned.htm

9. *December 21, Government Accountability Office* — **GAO−07−217R: Defense Contracting: Questions for the Record (Correspondence).** On September 7, 2006, David M. Walker, Comptroller General of the United States, testified before the Subcommittee on Defense Committee on Appropriations on recent trends in Department of Defense (DoD) contracting. Specifically, Walker testified about practices that undermine DoD's ability to establish sound business arrangements, particularly those involving the selection and oversight of DoD's contractors and their performance. The Subcommittee requested that he respond to a number of post−hearing questions relating to various issues, including measures that DoD can employ to ensure better contracting outcomes. Refer to source to view the questions and responses.
Source: http://www.gao.gov/new.items/d07217r.pdf

[Return to top]

Banking and Finance Sector

10. *December 22, Kyodo News (Japan)* — **Personal info of Nissan customers might have been leaked.** Nissan Motor Co said Thursday, December 21, that personal information of its customers, including their names and the vehicles they own, might have been leaked from its database. Nissan said that the number of customers whose information has been leaked has yet to be confirmed but that the database the company used from April 2003 to December 2005 contained such information as names, gender, and addresses of 5.38 million customers.
Source: http://www.japantoday.com/jp/news/394182

11. *December 21, News 4 Jacksonville (FL)* — **Thirteen charged, more wanted in $400,000 counterfeit check scheme.** Thirteen people were arrested and 16 more are wanted in what prosecutors said was a counterfeit check scheme that victimized Winn−Dixie, Public, Wal−Mart and other companies. The 29 people cashed 900 phony commercial checks worth almost $400,000 throughout Florida, Georgia, Alabama, South Carolina and Tennessee. "The shear volume of checks this group was doing is what really concerns people here," prosecutor Kevin Frein said. Investigators said data obtained from a recovered laptop computer in late 2005 led to an investigation nicknamed Operation Stop Payment that involved the state attorney's office, the U.S. Secret Service, the Florida Department of Law Enforcement and the Jacksonville Sheriff's Office. Frein said Lakeisha Williams and Fred Holliman were among there masterminds of the ring, which bought account numbers illegally from four local companies, printed fake payroll checks, then recruited dozens of people to cash them. Police said the crooks used financial software available for $70 at office supply stores to design the checks.
Source: http://news.yahoo.com/s/wjxt/20061221/lo_wjxt/10583211

12. *December 21, Reuters* — **SEC, Treasury to share money laundering info.** An information−sharing accord aimed at uncovering terrorist financing and money laundering was announced on Thursday, December 21, by the Department of the Treasury's financial crimes unit (FinCEN) and the Securities and Exchange Commission (SEC). Under the agreement, the SEC and FinCEN each quarter will share information they have gathered to make sure SEC−regulated companies comply with the Bank Secrecy Act. "The agreement will better ensure that SEC−regulated firms have robust anti−money laundering programs," the SEC said.

The SEC said the agreement will help authorities identify financial institutions with significant bank secrecy law violations or deficiencies and take enforcement and other action when needed. The announcement comes after U.S. financial authorities cited two international banks −−Habib Bank Ltd., one of Pakistan's largest banks, and Bank of Tokyo−Mitsubishi UFJ Ltd, the world's biggest bank in terms of assets −− for deficient anti−money laundering compliance procedures and internal controls.
Source: http://news.yahoo.com/s/nm/20061221/bs_nm/sec_moneylaunderin g_dc_1

13. *December 21, Baseline Magazine* — **Security Case: Washington Mutual addresses phishing.** Two years ago, Washington Mutual (WaMu) says, it was a popular target of phishers—scam artists who send e−mails to the Seattle−based bank's customers to entice them to give up their account information online. But now, a series of new security measures are giving phishers less of a return, and their numbers have declined. Dave Cullinane, WaMu's chief information security officer, says that for the last two years the bank has been working hard to fight phishers' work. WaMu took several steps to improve its own security, change the way it worked with customers, and share information with law enforcement and the financial services industry so that phishers would be less successful. WaMu recommends basing hardware and software on standard security controls approved by the National Institute of Standards and Technology; sharing information by keeping in touch with several industry groups, such as the Anti−Phishing Working Group, the Identity Theft Technology Council, BITS Financial Services Roundtable, and the Alliance for Enterprise Security Risk Management; ensuring that security is a bank−wide concern; learning to work with law enforcement; and not making customers feel bad when they fall for phishing scams.
Source: http://www.baselinemag.com/article2/0,1540,2070417,00.asp

14. *December 21, Customer Relationship Management News* — **Financial firms share security plans.** Anish Bhimani of JPMorgan Chase said the desire to avoid becoming another data−loss news story has prompted some changes, including adding laptop encryption and possibly adopting "tapeless" data centers. Some of the top players in the financial services arena −− such as Visa, JPMorgan Chase, and Experian −− are expanding their tactics for preventing customer data loss. IT security managers convening at two interrelated conferences in New York recently said their firms are adopting both new network defenses and organizational structures to lower risk of a data breach. Some say the very survival of their businesses may be at stake. Experian no longer accepts data that isn't encrypted, and uses a data−leak prevention appliance to monitor employee e−mail, file transfer and instant messaging. James Christiansen of Experian International is seeing trends in cybercrime by working with the U.S. Secret Service and others in the industry on Project Harvest. He sees that thieves around the world are selling software financial−theft Trojan programs for $1,000 to $5,000, a credit card with PIN for $500, and change of billing data for $80 to $300, and $7 to $25 depending on volume for stolen credit card numbers with security codes.
Source: http://www.crm−daily.com/story.xhtml?story_id=48926

[Return to top]

Transportation and Border Security Sector

15.

December 25, Associated Press — **Flights get back to full schedule at Denver airport.** On Sunday, December 24, hundreds of packed flights left the airport carrying passengers who had been stranded when a blizzard shut down the runways last week, wrecking the itineraries of holiday travelers around the country who raced to get home. Officials said they did not have a count of how many passengers remained at the airport on Christmas morning. They planned to distribute cots, but by early evening did not know if anyone stranded by the two−day snowstorm was still there. The airport's two biggest carriers, United and Frontier airlines, said they flew a full schedule Saturday and Sunday, including a dozen extra flights by United. Neither the airlines nor the airport had a passenger count. Last Christmas Eve, an estimated 129,000 passengers passed through the airport, the nation's fifth−busiest, but officials say patterns change from year to year. More than 3,000 incoming flights alone were canceled or diverted while Denver International was shut down for 45 hours after the storm hit Wednesday, December 20. Some passengers left for hotels or gave up and went home, but others stuck it out at the airport. An estimated 4,700 camped out there at the peak of the closure.
Source: http://www.usatoday.com/travel/news/2006−12−25−holiday−trave l_x.htm

16. *December 23, Associated Press* — **Records detail missing TSA badges, uniforms.** More than 3,700 identification badges and uniform items have been reported lost or stolen from Transportation Security Administration employees since 2003. Los Angeles International Airport reported the most items with 636 missing uniforms. O'Hare International Airport in Chicago reported 189 missing badges. Security experts have said the badges and uniforms could pose a security threat if they end up in the wrong hands.
Source: http://www.usatoday.com/travel/news/2006−12−22−tsa−badges−un iforms−missing−lost−stolen_x.htm

17. *December 23, Associated Press* — **Boston's Big Dig tunnel reopens.** The Big Dig's Interstate 90 westbound tunnel reopened late Saturday, December 23, after federal inspectors approved repairs made in the wake of motorist's death, a Massachusetts state official said. The road closed in July after concrete ceiling panels fell on a car, crushing 39−year−old Milena Del Valle. Workers have spent months testing and reinforcing bolts that keep the ceiling panels suspended above the roadway. The repairs, which are nearly complete, will cost an estimated $34 million, officials said this week. The $14.6 billion Big Dig −− the most expensive highway project in U.S. history −− has been plagued by problems and cost overruns throughout the two decades it's taken to design and build.
Source: http://www.usatoday.com/news/nation/2006−12−23−bigdig_x.htm

18. *December 22, New York Times* — **PATH tunnels seen as fragile in bomb attack.** An analysis done for the Port Authority of New York and New Jersey, based on work by Lawrence Livermore National Laboratory and the Rensselaer Polytechnic Institute, revises some critical aspects of an assessment of the PATH (Port Authority Trans−Hudson) system's vulnerability that was presented last spring. It makes clear that the tunnels −− four tubes of varying design and sturdiness that stretch across the Hudson riverbed −− are structurally more fragile than first thought. The four PATH tubes lie in the Hudson riverbed, not in bedrock The vulnerability of the PATH tubes and other tunnels has long been a source of concern to security, transportation and government officials, as well as the public. The fears have existed at least as far back as 1993, the year of the first terror attack on the World Trade Center. A 19−page summary of the analysis details some of the measures the Port Authority has been planning to put in place to

better secure the PATH system: laying concrete blankets atop the tubes to plug holes caused by a blast, strengthening portions of the tubes, and installing floodgates to prevent the system from being overwhelmed.
PATH Website: http://www.panynj.gov/CommutingTravel/path/html/index.html
Source: http://www.nytimes.com/2006/12/22/nyregion/22security.html?bl&ex=1166936400&en=c0e0b4a6ed7ff4ed&ei=5087

19. *December 21, NY1 News* — **"E−Zier Pass" could speed up commutes.** A pilot program in which straphangers can use the same bankcard, account−linked pass or cell phone to ride mass transit is reportedly in the works. The Metropolitan Transit Authority, Port Authority and New Jersey Transit are asking banks to come up with a system that lets customers use their bank or credit card like a MetroCard to pay for rides on subways, buses, trains and ferries. The new technology could also be installed on cell phones.
Source: http://www.ny1.com/ny1/content/index.jsp?stid=1&aid=65289

20. *December 21, Reuters* — **French film raises fresh fears over airport safety.** A French television reporter managed to smuggle explosive material and knives onto American and French passenger planes apparently revealing serious flaws in security at French airports. Appearing in a documentary made for state television, the reporter has raised fresh questions about French air safety after accusations last month that it was too easy to gain access to aircraft at Paris' main airport. Reporter Laurent Richard, aided by security expert Christophe Naudin, used hidden cameras to show themselves carrying "de−activated" Semtex explosive and a detonator in their hand luggage aboard an Air France flight to Nice. On another occasion, the pair carried two box cutters aboard a Delta airlines flight from Paris to New York, with security staff not looking at their screens as the weapons passed through the X−ray machines. Richard said the substance could not have exploded but had the same chemical characteristics of the plastic explosive Semtex, and should, in theory, have been detected. All the security breaches were made over the past month.
Source: http://today.reuters.com/news/articleinvesting.aspx?type=comktnews&storyID=2006−12−21T132138Z_01_L21742419_RTRUKOC_0_US−FRANCE−AIRPORT−SECURITY.xml&WTmodLoc=EntNewsIndustry_R1_comk tnews−1

21. *December 19, Department of Transportation* — **Secretary of Transportation opens federally funded hurricane resistant bridge to I−10 traffic over Florida's Escambia Bay.** A new eastbound bridge over Pensacola's Escambia Bay that is designed to survive the storm surges of a major hurricane is now open for traffic, Department of Transportation Secretary Mary E. Peters announced on Tuesday, December 19. The Secretary added that the bridge is needed to replace two lower spans that were destroyed by Hurricane Ivan in 2004. Secretary Peters said the $255.6 million cost of building the new bridge is 90 percent funded by the federal government. The Secretary added that traffic was expected to begin flowing on a second, similar westbound bridge across the bay later next year. She said the bridge opening now will address backups caused by the need to limit east−bound traffic on I−10 over the Bay to one lane after Hurricane Ivan caused significant damage to the bridge.
Source: http://www.dot.gov/affairs/dot11906.htm

[Return to top]

Postal and Shipping Sector

22. *December 22, KOIN (OR)* — **Suspicious powder found in mail.** Two letters containing a suspicious powder are being investigated after being received at two state agencies. Around noon on Friday, December 22, Oregon State Police responded to two separate reports of suspicious mail. One was received at the Oregon Department of Fish & Wildlife in Keizer, OR, and one at Capitol Hill in Salem. Police say appropriate safety precautions were taken to limit access to the buildings until the powder could be tested. In both cases, Salem Fire Department Hazardous Materials Team responded and determined the powder found in the mail was non−hazardous. Both buildings have returned to normal operations as evacuations were not necessary.
Source: http://www.koin.com/Global/story.asp?S=5851850

[Return to top]

Agriculture Sector

23. *December 22, Associated Press* — **South Korea rejects U.S. beef shipment.** South Korea has rejected the latest shipment of U.S. beef and asked Washington to explain why it contained unacceptable levels of the toxic chemical dioxin, a government official said Friday, December 22. According to a statement issued late Thursday, the South Korean Agriculture and Forestry Ministry found 6.26 picograms of the toxic substance in one gram of fat, part of a 10.2−ton shipment of U.S. beef which arrived on December 1. South Korean standards allow no more than five picograms per gram of fat. The discovery was the latest bad news for the U.S. cattle industry in South Korea, already dealing with the rejection of three recent shipments of beef for including banned bone fragments, which South Korea fears could potentially harbor bovine spongiform encephalopathy (BSE). Seoul barred U.S. beef in December 2003 after the first reported U.S. case of the BSE. Imports recently resumed after a nearly three−year ban, but so far no beef has made it to South Korean food stores or restaurants.
Source: http://sfgate.com/cgi−bin/article.cgi?f=/news/archive/2006/12/22/financial/f055011S40.DTL&type=business

24. *December 22, Canadian Press* — **Wyoming declared free of livestock disease that blocked exports to Canada.** Wyoming has been certified as being free of vesicular stomatitis (V.S.), a viral disease that affects horses, cattle and other livestock. Following the discovery of the disease this summer, Canada had put import restrictions on horses and cattle from Wyoming. Dr. Dwayne Oldham, Wyoming state veterinarian, announced Thursday, December 21, he now anticipates Canada will ease those restrictions. The U.S. Department of Agriculture notified the Wyoming Livestock Board the state is free of any quarantines for the disease. A horse on a ranch near the Natrona−Converse county line east of Casper, WY, tested positive for the disease in August. Vesicular stomatitis is a viral disease characterized by blister−like lesions on the mouths and tongues of horses, cattle and other livestock. It's transmitted by insects, so outbreaks typically subside in the winter. Although Wyoming is now certified to be free of V.S., Oldham said he still advises veterinarians to contact any state or other country before planning any interstate shipment of animals.
Source: http://www.canada.com/topics/news/agriculture/story.html?id=

70220a2c−c407−4132−b95e−bbd561fb6f10&k=27056

25. *December 22, South Florida Sun−Sentinel* — **Officials work to contain virus as fourth horse dies in Palm Beach County, Florida.** The deadly equine herpes virus sweeping Palm Beach County, FL's, western communities claimed another horse Thursday, December 21, as state officials seek control of the disease that has now killed four here, a fifth in California, and sickened eight others across Florida. A state official said a horse under quarantine at the Palm Beach Equine Clinic in Wellington, FL, developed neurological symptoms of the virus Thursday and quickly deteriorated. Officials set up a command center at the Palm Beach County Cooperative Extension Service outside West Palm Beach, FL, to gather information and track the spread of the virus. They also launched a toll−free hotline at 800−342−5869 for horse owners to report suspected cases or relay concerns to the state veterinarian's office. David Perry, a safety specialist with the Department of Agriculture who oversees inspectors from the command center, said they're collecting data that will help in the overall fight. Beyond that, he said, the best thing for the horses that show symptoms is isolation and monitoring.
Source: http://www.sun−sentinel.com/news/local/palmbeach/sfl−pvirus22dec22,0,6610276.story?coll=sfla−news−palm

26. *December 21, Successful Farming* — **Odds of Asian soybean rust striking the Midwest are lower than researchers first believed.** It may be too early for farmers to let their guards down, but at this point, the odds of Asian soybean rust striking the Midwest are lower than researchers first believed two years ago. Asian rust confirmation increased in the United States in 2006, as it was found in 15 states in a total 274 counties and parishes. However, massive rust infestations that many feared have not materialized as they have in Brazil. X. B. Yang, an Iowa State University plant pathologist cites the following reasons why rust fears have not yet materialized as they did in Brazil: the U.S. has more sunlight, less rain, a lower altitude, fewer strong wind currents, and a less hospitable host (kudzu) than in Brazil.
Source: http://www.agriculture.com/ag/story.jhtml;jsessionid=51KK54VN5FIBLQFIBQNSAOQ?storyid=/templatedata/ag/story/data/1166731165918.xml&catref=ag1001

27. *December 21, Orlando Sentinel (FL)* — **Researchers tout new test to detect threats to citrus.** The next time a disease such as citrus canker or greening surfaces in Florida or elsewhere, scientists should have a far easier time getting a quick fix on the culprit. Researchers are buzzing about the potential for a new test said to be far faster and more thorough than existing screening techniques. The new tool, called TIGER −− short for Triangulation Identification for Genetic Evaluation of Risks −− will help scientists who are on the lookout for potentially dangerous diseases. Researchers say the new TIGER test is a significant advance in the detection field as the threat of bioterrorism, and economically damaging "agroterrorism," grows. Using fragments of nucleic acid called primers, the technique identifies a range of pathogens within minutes.
Source: http://www.orlandosentinel.com/business/orl−citrustest2106dec21,0,783090.story?coll=orl−business−headlines

[Return to top]

Food Sector

28. *December 22, Canadian Press* — **National warning issued in Canada after metal pins found in cooked turkey.** The federal food watchdog and a Manitoba−based poultry co−operative have issued a warning to the public after metal pins were found in a turkey cooked at an Ottawa−area home. The Canadian Food Inspection Agency and Granny's Poultry Co−operative (Manitoba) Ltd. say the consumer found the pins while slicing the bird; no injuries were reported and a police investigation has begun. Authorities say no other pins were found after inspecting 505 packaged turkeys from the Ottawa retail store and a Manitoba warehouse; they say evidence so far indicates a "very high probability" it is an isolated incident.
Source: http://www.cbc.ca/cp/health/061222/x122204A.html

[Return to top]

Water Sector

29. *December 22, WETM 18 (NY)* — **E. coli and Coliform found in drinking water in Horseheads, New York.** E. Coli and Coliform bacteria have been found in the water supply in the Village of Horseheads, New York. More than 10,000 people were told, Friday, December 22, to boil their water if they plan on consuming it. The order will remain in effect for at least two days, until tests show the water is safe to drink. The boil water order only affects people whose water comes from the Village of Horseheads; people who get their water from private wells or other municipal systems are not affected. The entire Horseheads School District was dismissed. Students were taken to their designated emergency locations.
Source: http://www.wetmtv.com/news/local/story.aspx?content_id=69274ED8−EC0C−4A87−A28F−8FE8FE19AB33

30. *December 21, Environmental Protection Agency* — **EPA to require monitoring for unregulated contaminants.** Approximately 4,000 public water systems will monitor drinking water for up to 25 unregulated chemicals to inform the Environmental Protection Agency (EPA) about the frequency and levels at which these contaminants are found in drinking water systems across the United States. The information will help determine whether regulations are needed to protect public health. This is the second scheduled review under the Unregulated Contaminant Monitoring Rule (UCMR 2). EPA currently has regulations for more than 90 contaminants. The Safe Drinking Water Act requires EPA to identify up to 30 contaminants for monitoring every five years. The first cycle, UCMR 1, was published in 1999 and covered 25 chemicals and one microorganism. The new rule requires systems to monitor for contaminants that are not regulated under existing law. More information about the UCMR 2 rule: http://epa.gov/safewater/ucmr/ucmr2 or call the Safe Drinking Water Hotline at 800−426−4791.
Source: http://yosemite.epa.gov/opa/admpress.nsf/27166bca9a9490ee852570180055e350/7d26e0c3e732b4388525724b0051f201!OpenDocument

[Return to top]

Public Health Sector

31. *December 23, Associated Press* — **Third norovirus outbreak sickens 54 at nursing home.** The third suspected norovirus outbreak in the Lansing, MI, area in the past month has affected 54 people at a nursing home. The Courts of Holt has closed its doors to new patients and most visitors, the Lansing State Journal reported Friday, December 22. About half of the home's 81 residents and 12 employees have experienced vomiting and diarrhea, two of the main symptoms from norovirus. The Delta Retirement Center in Delta Township reported a similar outbreak in the past few weeks, affecting more than 60 people. In late November and early December, at least 36 people got sick from an outbreak at an Applebee's restaurant in Delta Township. The cases don't appear to have a common link.
Source: http://www.freep.com/apps/pbcs.dll/article?AID=/20061223/NEWS05/612230379

32. *December 22, Nature* — **Prions removed from animal blood.** A U.S.−led research team has developed a technique to filter potentially deadly prion proteins from blood. They suggest that the method should be used routinely in attempts to remove prions, which can cause variant Creutzfeldt−Jakob disease (vCJD), from blood products used for transfusions. Routine filtering of blood to remove any prions would sidestep the danger, say the researchers, led by Robert Rohwer of the University of Maryland, Baltimore. He and his colleagues searched databases of millions of molecules to find ones that bind to the prion protein. They eventually identified a resin, called L13, that binds to both the normal and disease−causing forms. They tested the resin using hamster blood spiked with the prions that cause scrapie, a disease related to vCJD. They then used this blood to transfuse hamsters. Around half of the animals injected with untreated blood developed disease, but the nearly 200 hamsters injected with blood filtered with L13 remained disease−free. The problem is that effectiveness of the filtration will be very difficult to verify in people, because although there is a test for infective prions in hamster blood, no such test yet exists for humans.
Report summary: http://www.thelancet.com/journals/lancet/article/PIIS0140673606698978/abstract
Source: http://www.nature.com/news/2006/061218/full/061218−13.html

33. *December 21, Integrated Regional Information Networks* — **Health experts battle unknown disease outbreaks in Angola.** Health organizations in Angola are scrambling to identify a disease that has surfaced in Uige Province, in the north, and in Huila Province, in the south, to prevent further transmission and treat fatally ill patients −− half of whom have already died. "We have seen more than 35 cases since November and 50 percent of the patients were dying," said Karen Godley, head of mission in Angola for Medecins Sans Frontieres (MSF)−Switzerland. Although located at opposite ends of Angola, Uige and Huila both have a growing number of patients with symptoms like "bloody diarrhea", Godly said. "We have no idea what we are dealing with −− there is an urgency to identify the pathogen to protect communities and health workers, and to provide the best treatment for patients." Of the 16 cases in Uige, six have been fatal, according to Monica Camacho, head of mission in Angola for MSF−Spain. "There are few patients, but the fatality rate is high." Health organizations are still in the dark as to how the disease is spread. According to Dr. Satounata Diallo, World Health Organization country representative in Angola, "this is not Ebola or Marburg."
Source: http://www.irinnews.org/report.asp?ReportID=56814&SelectRegion=Southern_Africa&SelectCountry=ANGOLA

34.

December 21, Associated Press — **New flu pandemic could kill 81 million.** A flu virus as deadly as the one that caused the 1918 Spanish flu could kill as many as 81 million worldwide if it struck today, a new study estimates. By applying historical death rates to modern population data, the researchers calculated a death toll of 51 million to 81 million, with a median estimate of 62 million. That's surprisingly high, said lead researcher Chris Murray of Harvard University. He did the analysis, in part, because he thought prior claims of 50 million deaths were wildly inflated. One surprise in the new study was the huge variation in how different countries would be affected by a pandemic. The study estimates that 96 percent of the deaths would occur in the developing world. Murray and colleagues noted there was a 30−fold or more variation in mortality. "That tells us it's not just the genetic makeup of the virus that will cause deaths, but that there are a lot of other things that intervene," he said. Determining the mitigating factors might help avert a catastrophe. "If we can answer that question, we may unlock the mysteries behind which non−pharmaceutical strategies could significantly decrease mortality," said Murray.
Study: http://www.thelancet.com/journals/lancet/article/PIIS0140673 606698954/fulltext
Source: http://news.yahoo.com/s/ap/20061222/ap_on_he_me/flu_pandemic

35. *December 21, Government Health IT* — **Many agencies to contribute to pandemic preparedness.** The federal government is tapping the expertise of agencies and departments including the Defense Threat Reduction Agency (DTRA) and the Bureau of Justice Assistance to help manage the domestic response to a pandemic flu outbreak, according to a new report from the Department of Health and Human and Services (HHS). The report is an update to the National Strategy for Pandemic Influenza plan the Bush administration released last November. According to HHS, overseas federal agencies are working with the World Health Organization and countries with outbreaks of the H5N1 flu virus to bolster human and animal disease surveillance networks. For example, HHS is staffing the Regional Emerging Disease Infection Center in Singapore. DTRA, which has a primary mission of safeguarding the country against weapons of mass destruction attack, has provided modeling tools for real−time epidemic analysis, making it possible to study public health and emergency preparedness for handling a pandemic flu outbreak, the HHS report states.
National Pandemic Plan Progress Report:
http://www.pandemicflu.gov/plan/federal/stratergyimplementat ionplan.html
Source: http://www.govhealthit.com/article97175−12−21−06−Web

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

36. *December 24, Xinhua* — **China holds state−level anti−terrorist exercise.** China launched its third state−level anti−terrorist exercise, involving both military and civil departments in the response to a terrorist biochemical attack on Saturday, December 23. The exercise, dubbed

Great Wall No. 3, began at 10 a.m. in Qingdao city in east China's Shandong Province but was coordinated from Beijing. The exercise, based on terrorist attack scenarios, focused on the city's emergency response and its capacity to mobilize anti−terrorism forces. Contrary to two previous exercises, the target city was not revealed beforehand and no rehearsals for the attack were carried out. As soon as the simulated biochemical attack began, a local headquarters was set up to muster and dispatch emergency forces, a pattern which is expected to serve as a model for Chinese cities in future anti−terrorist work. Zhou Yongkang, State Councilor and Minister of Public Security, who commanded the drill, said that the exercise was a means of testing emergency security systems in advance of the 2008 Beijing Olympic Games. China held a state−level anti−terror drill dubbed "Great Wall 2003" in September 2003 and "Great Wall No. 2" in January 2006.
Source: http://english.people.com.cn/200612/24/eng20061224_335361.ht ml

37. *December 22, Government Accountability Office* — **GAO−07−44: Transportation−Disadvantaged Populations: Actions Needed to Clarify Responsibilities and Increase Preparedness for Evacuations (Report).** The evacuation of New Orleans in response to Hurricane Katrina in 2005 raised questions about how well state and local governments, primarily responsible for disaster planning, integrate transportation−disadvantaged populations into such planning. The Government Accountability Office (GAO) assessed the challenges and barriers state and local officials face; how prepared these governments are and steps they are taking to address challenges and barriers; and federal efforts to provide evacuation assistance. GAO reviewed evacuation plans; Department of Homeland Security (DHS), Department of Transportation (DOT), and other studies; and interviewed officials in five major city and four state governments. DHS should clarify federal agencies' roles and responsibilities for providing evacuation assistance when state and local governments are overwhelmed. DHS should require state and local evacuation preparedness for transportation−disadvantaged populations and improve information to assist these governments. DOT should encourage its grant recipients to share information to assist in evacuation preparedness for these populations. DOT and DHS agreed to consider our recommendations, and DHS stated it has partly implemented some of them.
Highlights: http://www.gao.gov/highlights/d0744high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−44

[Return to top]

Information Technology and Telecommunications Sector

38. *December 22, eWeek* — **Vista exploit surfaces on Russian hacker site.** Proof−of−concept exploit code for a privilege escalation vulnerability affecting all versions of Windows −− including Vista −− has been posted on a Russian hacker forum, forcing Microsoft to activate its emergency response process. Mike Reavey, operations manager of the Microsoft Security Response Center (MSRC), confirmed that the company is "closely monitoring" the public posting, which first appeared on a Russian language forum on December 15. It affects "csrss.exe," which is the main executable for the Microsoft Client/Server Runtime Server. According to an alert cross−posted to security mailing lists, the vulnerability is caused by a memory corruption when certain strings are sent through the MessageBox API. "The PoC reportedly allows for local elevation of privilege on Windows 2000 SP4, Windows Server 2003

SP1, Windows XP SP1, Windows XP SP2 and Windows Vista operating systems," Reavey said in an entry posted late Thursday, December 21, on the MSRC blog.
MSRC blog: http://blogs.technet.com/msrc/archive/2006/12/22/new−report−of−a−windows−vulnerability.aspx
Source: http://www.eweek.com/article2/0,1895,2076062,00.asp

39. *December 22, Sophos* — **CafePress Website struck by distributed denial−of−service attack.** Sophos has reminded companies of Internet attacks after popular Website CafePress.com told its members that it is currently the victim of a distributed denial−of−service (DDoS) assault. CafePress.com is a Website that allows Internet users to set up their own online store to easily sell customized merchandise such as t−shirts, mugs and coasters. CafePress.com handles the Website hosting, order fulfillment and payment processing on behalf of the store owner. DDoS attacks are used by Internet hackers to disrupt Websites, flooding them with traffic from zombie computers and making them inaccessible for the general public. Sophos experts speculate that the hackers may have deliberately targeted CafePress.com in the run−up to the holidays, as it is a prime shopping period.
Source: http://www.sophos.com/pressoffice/news/articles/2006/12/cafe press.html

40. *December 22, TechWeb* — **Sale of voting machine firm with Venezuelan links will avoid U.S. probe.** Voting machine provider Smartmatic Corp. and its Venezuelan owners will avoid a full U.S. national security investigation by putting the firm's Sequoia Voting Systems Inc. U.S. subsidiary up for sale. Attention has been focused on the firm because of reports it has had business connections with the government of Venezuelan President Hugo Chavez, who frequently attacks U.S. policy. In an announcement Friday, December 22, Smartmatic said it has withdrawn from a review process that was scheduled to be carried out by the U.S. Committee on Foreign Investment in the United States (CFIUS), which reviews foreign investments and acquisitions to determine whether they hold national security threats. The CFIUS investigation was examining whether Smartmatic and Sequoia had or continue to have any connection to the Chavez government.
Source: http://www.techweb.com/showArticle.jhtml;jsessionid=YIRI02RIVH0LCQSNDLRCKHSCJUNN2JVN?articleID=196701695

41. *December 22, IDG News Service* — **Santa's Website hacked.** The consumer advocacy group StopBadware.org said it was approached last week by an Incline Village, NV, man who has legally changed his name to Santa Claus, who asked them to help figure out why his Website was being flagged by Google Inc.'s Website filters. It turned out that Santa's Website, Santaslink.net had been hacked. "Nestled all snug in the bottom of his homepage was a nice little bit of code containing a badware link," said StopBadware.org Developer Jason Callina.
Source: http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_hacking&articleId=9006639&taxonomyId=82&intsrc=kc_top

42. *December 21, TechWorld (UK)* — **Spam project pulls the plug.** Anti−spam blacklist service, The Open Relay Database (ORDB), has pulled the plug after five and a half years because of spammers' growing sophistication. ORDB was designed to deal with a technique in which spammers used SMTP proxy servers to flood the Internet with junk e−mail. The project distributed a blacklist of mail servers that allowed third−party relay −− "open relays" −− and

were thus liable to be used by spammers. But the list had leveled off at around 225,000 over the past year and updates have slowed to a crawl, the volunteer−run project acknowledged. ORDB is essentially a victim of its own success −− five years ago around 90 percent of spam was sent through open relays, and now the figure is less than one percent, due to blocking lists and to ISPs disallowing third−party relay. Spammers haven't been deterred and generally now rely on botnets to send spam.
Source: http://www.techworld.com/networking/news/index.cfm?newsID=76 53&pagtype=all

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 15901 (−−−), 6881 (bittorrent), 1027 (icq), 4662 (eDonkey2000), 4672 (eMule), 1028 (−−−), 445 (microsoft−ds), 25 (smtp), 42625 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

43. *December 25, Associated Press* — **Two in custody after deadly Florida mall shooting.** Two men were in custody Monday, December 25, after a shooting at a crowded mall tin Boynton Beach, FL, hat left one man dead and sent hundreds of Christmas shoppers running for cover, police said. Jesse Cesar, 21, was charged with first−degree murder and attempted first−degree murder of a police officer. Cesar fatally shot Berno Charlemond, 23, at the Boynton Beach Mall, north of Miami, on Sunday afternoon, Police Lt. Jeffrey Katz said. Cesar fled, firing at police as he led them on a chase through the mall, Katz said. Officers did not return fire and no one else was injured. SWAT team members arrested Cesar after he barricaded himself in part of a Dillard's store and refused to surrender, Katz said. Fregens Daniel, 20, of Boynton Beach, also was arrested and was charged with acting as principal accessory in the case, Katz said. Police did not disclose the number of shots fired. A motive for the shooting has not been determined, but Katz said Charlemond, of Boynton Beach, was arrested a month ago at the same mall for carrying a concealed weapon. A mall spokesperson, Sam Yates, said the shooting occurred outside of a store. The mall was evacuated and remained closed the rest of the day.
Source: http://hosted.ap.org/dynamic/stories/M/MALL_SHOOTING?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

44. *December 23, Savannah Morning News (GA)* — **Police seize German grenades from Georgia mobile home.** A man was in jail Friday, December 22, after police seized explosives from his mobile home. The Savannah−Chatham Metropolitan Police Bomb Squad was sent to Skidaway Mobile Estates on Thursday following a report of explosives. Officers searched the mobile home and found several suspicious items stored inside a homemade gun cabinet in a bedroom, police spokesperson Sgt. Mike Wilson said. Officers seized several canisters containing

explosive−making materials, including German military grenades, igniters, fuses, and consumer fireworks, Wilson said. The explosives will be sent to the Georgia Bureau of Investigation crime lab to determine their composition, police said. Police arrested the home's owner, Patrick Glisson, on charges of possession of an explosive device with intent to distribute.
Source: http://savannahnow.com/node/200960

[Return to top]

General Sector

Nothing to report.
[Return to top]